

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF OHIO  
EASTERN DIVISION

|                           |   |                      |
|---------------------------|---|----------------------|
| UNITED STATES OF AMERICA, | ) | CASE NO. 1:16-CR-265 |
|                           | ) |                      |
| Plaintiff,                | ) |                      |
|                           | ) | JUDGE JOHN ADAMS     |
| -vs-                      | ) |                      |
|                           | ) |                      |
| ERICK HENDRICKS,          | ) |                      |
|                           | ) |                      |
| Defendant.                | ) |                      |

**DEFENDANT ERICK HENDRICKS MOTION TO FOR DISCLOSURE OF FISA-RELATED MATERIAL AND TO SUPPRESS THE FRUITS OR DERIVATIVES OF ELECTRONIC SURVEILLANCE**

Defendant, Erick Hendricks, respectfully moves this Court, pursuant to the Free Exercise, Free Speech, Search and Seizure, Due Process and Effective Assistance of Counsel clauses of the First, Fourth, Fifth and Sixth Amendments to the Constitution of the United States, as well as the relevant provisions of the Foreign Intelligence Surveillance Act (“FISA”), specifically including 50 U.S.C. § 1806(e)-(g), hereby moves for disclosure of FISA-related materials; and to suppress any fruits or derivatives of electronic surveillance and any other means of collection conducted pursuant to FISA or any other foreign intelligence gathering. The specific bases for suppression include, but are not limited to the following:

- (1) FISA application(s) for electronic surveillance of Defendant’s e-mail accounts may fail to establish probable cause that Defendant, or whomever was targeted, was “an agent of a foreign power;”
- (2) The FISA application(s) may contain intentional or reckless material falsehoods or omissions, and therefore may violate the Fourth Amendment principles identified in *Franks v. Delaware*, 438 U.S. 154 (1978);
- (3) The primary purpose of the electronic surveillance was to obtain evidence of domestic criminal activity and not foreign intelligence information, or, conversely, capturing foreign intelligence information was not a “significant”

purpose of the FISA surveillance;

- (4) The FISA surveillance may have been based impermissibly on activity protected by the First Amendment;
- (5) The government may not have made the required certifications in the FISA application(s), or may have failed to obtain necessary extensions of prior FISA orders, or continued the FISA surveillance after any basis for such initial surveillance was no longer valid;
- (6) The government may not have established or abided by the appropriate minimization procedures required by FISA;
- (7) The government may have violated other provisions of FISA and/or the First and/or Fourth Amendments in manners unknown to the Hendricks.

Hendricks' argument is more fully explained in the attached memorandum.

Respectfully submitted,

S/Stephen D. Hartman  
Stephen D. Hartman (OH 0074794)  
310 River Road  
Maumee, OH 43537  
(419) 461-6107  
(419) 710-0496 Fax  
stevehartmanlaw@gmail.com

S/ David L. Doughten  
David L. Doughten (OH 0002847)  
4403 St. Clair Ave.  
Cleveland, OH 44103  
(216) 361-1112  
(216) 881-3928 Fax  
ddoughten@yahoo.com

COUNSEL FOR DEFENDANT ERICK JAMAL HENDRICKS

**CERTIFICATE OF SERVICE**

I hereby certify that on the 28th of July, 2017 a copy of the foregoing was filed electronically. Parties may access this filing through the Court's system. Notice of this filing will be sent by operation of the Court's electronic filing system

S/ David L. Doughten  
David L. Doughten

Attorney for Defendant Hendricks

## MEMORANDUM IN SUPPORT

### I. OVERVIEW

On August 17, 2016, the Government indicted Hendricks and in a one counts for one count providing material support and resources to a foreign terrorist organization including the Islamic State of Iraq and Levant (ISIL), knowing that ISIL had been designated by the Secretary of State as a foreign terrorist organization. (Dkt. 7) A superseding indictment was filed on December 13, 2016. This indictment included an additional charge of Conspiracy to Provide Material Support and Resources to a Foreign Terrorist Organization. (Dkt. 25)

Discovery tendered by the government has revealed voluminous emails, electronic communications, and other online activity involving Hendricks. These electronic communications include emails from several email accounts, among telephone, bank, and other records. While it is unclear when the government's use of FISA surveillance began and such details have not been disclosed, the Indictment and discovery indicate early implementation of that surveillance. Indeed, the indictment includes email communications from as early as 2005. (See, *e.g.*, Indictment, ¶ 6) Thus, based upon the discovery and the allegations in the Indictment, it appears that surveillance of Defendant's online activity may very well have lasted from sometime before December 1, 2014 through May of 2015. Although without access to any of the FISA or foreign intelligence surveillance applications and warrants, counsel can only assume this to be true.

Thus, while it is unclear precisely which electronic communications were collected pursuant to FISA and over what exact time period, as discussed in detail below, the numerous e-mails, online activity, and other electronic information that the government presumably obtained

pursuant to FISA must be suppressed because the surveillance and/or collection violated the provisions of FISA, as well as principles of the First and Fourth Amendments. In light of the fact that FISA governs searches on U.S. soil, the Fourth Amendment is clearly implicated.

However, because defense counsel have not been provided with the underlying applications for the pertinent FISA warrants, this motion can only outline the possible bases for suppression for the Court to examine and consider. Counsel therefore respectfully request that the Court:

- a) review all applications for electronic surveillance of the defendant conducted pursuant to FISA;
- b) order the disclosure of the applications for the FISA warrants to Defendant's counsel pursuant to an appropriate protective order;
- c) conduct an evidentiary hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978); and,
- d) as a result, suppress all FISA intercepts and seizures, and fruits thereof, derived from illegally authorized or implemented FISA electronic surveillance.

## II. THE HISTORY, PURPOSES, AND PROVISIONS OF FISA

In 1975, Congress established a committee to investigate allegations of “substantial wrongdoing” by the intelligence agencies in their conduct of surveillance. *Final Report of the S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities (Book II)*, S. Rep. No. 94-755, at v (1976) (“Church Report”). The committee discovered that, over the course of four decades, the intelligence agencies had “violated specific statutory prohibitions,” “infringed the constitutional rights of American citizens,” and “intentionally disregarded” legal limitations on surveillance in the name of “national security.” *Id.* at 137. Of particular concern to the committee was that the agencies had “pursued a ‘vacuum cleaner’ approach to intelligence

collection,” in some cases intercepting Americans’ communications under the pretext of targeting foreigners. *Id.* at 165. To ensure proper judicial involvement in the protection of Americans’ communications, the committee recommended that all surveillance of communications “to, from, or about an American without his consent” be subject to a judicial warrant procedure. *Id.* at 309.

In 1978, FISA, 50 U.S.C. §1801, *et seq.*, was enacted. The statute was designed to provide a codified framework for foreign intelligence gathering within the confines of the United States in response to civil liberties concerns and the gap in the law noted by the Supreme Court in *United States v. United States District Court*, 407 U.S. 297, 308-09 (1972).

Through FISA, Congress attempted to limit the propensity of the Executive Branch to engage in abusive or politically-motivated surveillance. FISA constituted Congress’ attempt to balance the “competing demands of the President’s constitutional powers to gather intelligence deemed necessary to the security of the Nation, and the requirements of the Fourth Amendment.” H.R. Rep. No. 95-1283, at 15. As a result, FISA’s provisions represented a compromise between civil libertarians seeking preservation of Fourth Amendment and privacy rights, and law enforcement agencies citing the need for monitoring agents of a foreign power operating in the United States. *See In re Kevork*, 788 F.2d 566, 569 (9th Cir. 1986) (FISA “was enacted in 1978 to establish procedures for the use of electronic surveillance in gathering foreign intelligence information . . . The Act was intended to strike a sound balance between the need for such surveillance and the protection of civil liberties”) (quotation omitted). Since its inception, FISA’s constitutionality has been upheld without exception.<sup>4</sup>

Important differences exist between the standards for a FISA warrant and that issued

under the Fourth Amendment and/or Title III of the U.S. Criminal Code; including that the “probable cause” required under FISA is merely that the target qualifies as an “agent of a foreign power,” and that the “agent of a foreign power” will use the electronic device subject to electronic surveillance, or owns, possesses, uses, or is in the premises to be searched. Thus, as the Ninth Circuit explained in *United States v. Cavanagh*, 807 F.2d 787 (9th Cir. 1987), “[w]ith important exceptions not pertinent here, FISA requires judicial approval before the government engages in any electronic surveillance for foreign intelligence purposes.” *Id.* at 788.

FISA also requires that any application to the FISA Court be made under oath by a federal officer and contain certain information and certifications found in §1804, which, in summary, are as follows:

- (1) The FISA application must provide the identity of the federal officer making the application. §1804(a)(1);
- (2) The FISA application must identify or describe the target. §1804(a)(2);
- (3) The FISA application must contain “a statement of the facts and circumstances relied upon by the applicant to justify his belief that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power and each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used by a foreign power or an agent of a foreign power[.]” §1804(a)(3). *See United States v. Posey*, 864 F.2d 1487, 1490 (9th Cir. 1989). FISA defines the term “foreign power,” in pertinent part as “a group engaged in international terrorism or activities in preparation therefor.” §1801(a)(4);
- (4) The application to the FISC must provide a “statement of the proposed minimization procedures.” §1804(a)(4);
- (5) The FISA application must include a “description of the nature of the information sought and the type of communications or activities to be subjected to surveillance.” §1804(a)(5). Thus, FISA appears to require that both the information sought *and* the communications subject to surveillance would have to relate directly to activities involving both an agent of a foreign power and international terrorism as defined in FISA;

- (6) The FISA application must include certain “certifications,” enumerated in §1804(a)(6)(A)-(E), and made by designated government officials, that:
  - (A) the certifying official deems the information sought to be foreign intelligence information;
  - (B) the purpose of the surveillance is to obtain foreign intelligence information;
  - (C) such information cannot reasonably be obtained by normal investigative techniques;
  - (D) designates the type of foreign intelligence information being sought according to the categories describe in” §1801(e); and
  - (E) includes a statement of the basis for the certification that –
    - (i) the information sought is the type of foreign intelligence information designated; and
    - (ii) such information cannot reasonably be obtained by normal investigative techniques.
- (7) The FISA application must contain a statement of the means by which surveillance will be effected and a statement whether physical entry is required to effect the surveillance. §1804(a)(7);
- (8) The FISA application must contain a statement of facts listing all previous related FISA applications made to any FISC judge, and action taken on each previous application. §1804(a)(8); and
- (9) The FISA application must specify the period of time for which the electronic surveillance is required to be maintained. §1804(a)(9).

In addition, the Attorney General must personally review the application and determine whether it satisfies the criteria and requirements set forth in FISA. § 1804(d); *see* § 1805(a)(1).

Regarding the judicial component of the FISA process, in considering an application for electronic surveillance pursuant to FISA, the Court should reject the application unless the application meets the following criteria sufficient to permit the Court to make the requisite findings under §1805(a):

- (i) that the application was made by a federal officer and approved by the Attorney General;

- (ii) that there exists probable cause to believe that “the target of the electronic surveillance is a foreign power or an agent of a foreign power . . . and . . . each of the facilities or places at which the electronic surveillance is directed is being used or is about to be used by a foreign power or agent of a foreign power[;]”
- (iii) that the proposed minimization procedures meet the definition of minimization procedures under §1801(h); and,
- (iv) that the application contains all required statements and certifications.

Also, in accordance with §1805(a)(4), if a target is a “United States person,” the FISC must determine whether the “certifications” under §1804(a)(6)(E)—namely that the information sought is “the type of foreign intelligence information designated,” and the information “cannot reasonably be obtained by normal investigative techniques”—are “not clearly erroneous.”

In addition, §1805(a)(2)(A) provides “that no United States person may be considered a foreign power . . . solely upon the basis of activities protected by the First Amendment.” Critical to the operation of FISA and its application in this case are the definitions related to “foreign power” set forth in 50 U.S.C. § 1801. A “foreign power” is defined in § 1801(a) to include foreign governments, groups they control, and groups engaged in terrorism. An “Agent of a foreign power” is defined as any person who:

- (A) Knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
- (B) Pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

- (C) Knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
- (D) Knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or,
- (E) Knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

50 U.S.C. §1801(b)(2).

Orders authorizing FISA wiretaps are issued for certain specified periods of time, but can be extended pursuant to additional applications. §§1805(d)(1) & (2). FISA authorizes any “aggrieved person” to move to suppress evidence obtained or derived from an electronic surveillance on the grounds that “the information was unlawfully acquired” or “the surveillance was not made in conformity with an order of authorization or approval.” §§1806(e)(1) & (2); 1825(f). FISA defines “aggrieved person” as “a person who is the target of electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.” §1801(k). FISA permits evidence generated in intelligence investigations to be used in criminal prosecutions. §§1806(b) & 1825(c).

### **III. DEFENDANT’S CHALLENGES TO THE FISA ELECTRONIC SURVEILLANCE IN THIS CASE**

Counsel cannot address any specific content or details of any of the FISA applications in this case because those applications have not been provided to counsel. While aggrieved criminal defendants, like Hendricks, may move to suppress FISA-generated evidence, §1806(f) provides

that if the Attorney General files an affidavit that “disclosure or an adversary hearing would harm the national security of the United States,” the court deciding the motion must consider the application and order for electronic surveillance *in camera* to determine whether the surveillance was conducted lawfully. As addressed in more detail below, § 1806(f) provides:

[i]n making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

Alternatively, §1806(g) provides that “[i]f the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.”

Here, although the defense has not been notified whether the Attorney General has yet submitted an affidavit under §1806(f), it is assumed for purposes of this motion that the government has or will make such a filing, and the arguments presented below in favor of suppression are made in anticipation of such a filing and the government’s position that *ex parte* proceedings are necessary. Thus, the grounds for relief set forth below represent defense counsel’s best estimation of the deficiencies in the FISA electronic surveillance in this case.

It goes without saying that the lack of access to the underlying FISA materials presents significant impediment to any defendant’s capacity to challenge FISA surveillance with much particularity. As the Fourth Circuit recognized in a closely analogous context—discerning what exculpatory evidence a witness solely within the government’s control, and to whom the defense is denied access, can provide—when a defendant is deprived of such access, the burden to be specific with respect to the material in question must be relaxed accordingly. *See United States v.*

*Moussaoui*, 382 F.3d 453, 472 (4th Cir. 2004), *citing United States v. Valenzuela-Bernal*, 458 U.S. 858, 870-71, 873 (1982).

Although moving to suppress FISA materials may be, in fact, an exercise in futility, Hendricks must nevertheless push for protection for abuse from this Court. From the time of FISA's inception in 1978, disclosure of FISA materials to defense counsel has never been deemed necessary, except for one instance, *United States v. Daoud*. *See United States v. Daoud*, No. 12–CR–723, 2014 WL 321384, at \*3 (N.D. Ill. Jan 29, 2014). Judge Coleman's decision was promptly reversed by the Seventh Circuit. *See United States v. Daoud*, 755 F.3d 479 (7th Cir. 2014).

**A. The FISA Applications Failed to Establish the Requisite Probable Cause.**

**1. The Elements of Probable Cause under FISA.**

Before authorizing FISA surveillance, the FISA Court must find, *inter alia*, probable cause to believe that “the target of the electronic surveillance is a foreign power or an agent of a foreign power.” §1805(a)(2)(A). The Supreme Court has reiterated the long-standing rule that criminal probable cause requires “a reasonable ground for belief of guilt,” and that “the belief of guilt must be particularized with respect to the person to be searched or seized.” *Maryland v. Pringle*, 540 U.S. 366, 371 (2003). Under FISA, though, unlike a traditional warrant, the probable cause standard is directed *not* at the target's alleged commission of a crime, but at the target's alleged status as “a foreign power or an agent of a foreign power.

**2. The “Agent of a Foreign Power” Requirement.**

Consequently, this Court must initially determine, with respect to each application for

FISA electronic surveillance of Hendricks, whether the application established a reasonable, particularized ground for belief that Hendricks qualified as an “agent of a foreign power.” §§1805(a)(2)(A) & 1801(b)(2)(C) & (E). As set forth above, FISA provides several definitions for an “agent of a foreign power,” and multiple definitions for a “foreign power.” These definitions include a requirement that a person’s activities are or may be in violation of the criminal laws of the United States. 50 U.S.C. §§ 1801(b)(2)(A) and (B), (c)(1), and (d). The need to establish a relationship to criminal activity for United States persons is made clear by the legislative history of FISA. H.R. Rep. 95-1283, Pt. 1 at 36, 95th Cong., 2d Sess. 21 (1978). One of the only decisions issued by the Foreign Intelligence Court of Review (“FISCR”), which is the appellate court for the FISC, underscored this point when it noted that the definition of agent of a foreign power for United States persons “is closely tied to criminal activity.” *In re Sealed Case*, 310 F.3d 717, 738 (FISA Ct. Rev. 2002).

Here, absent an opportunity to review the applications for any of the surveillance orders at issue, the defense counsel cannot specify whether the allegations asserting that Hendricks, or whoever was the target of the surveillance, was an “agent of a foreign power” were sufficient to satisfy FISA.

Because FISA requires proof of criminal activity to support surveillance or search of a United States person, significant questions may also arise involving the interplay between the FISA standard and the long-standing rules that probable cause requires “a reasonable ground for belief of guilt” and “the belief of guilt must be particularized with respect to the person searched or seized.” *See Maryland v. Pringle*, 540 US. 366, 371 (2003). Thus, in addition to providing grounds for suppression, the involvement of defense counsel will be necessary to counter

arguments the government likely made in support of the validity of any FISA application or warrant.

### **3. The Nature and Origins of the Information in the FISA Applications.**

Again, unlike the perfunctory disclosure of traditional warrants, the non-disclosure of the FISA applications denies the defense the ability to contest the accuracy and/or reliability of the underlying information used to satisfy FISA's version of probable cause. As a result, absent such disclosure, Hendricks can request only that the Court review the FISA applications with a degree of cognizance of certain factors and principles.

#### ***a) The Limits of "Raw Intelligence."***

For example, foreign intelligence information is often in the form of "raw intelligence," and not vetted in the manner typical of information law enforcement agents supply in ordinary warrant applications, *i.e.*, that the information emanated from a source that was reliable and/or had a verifiable track record, or was independently corroborated. Such raw intelligence is often not attributed to *any* specific source, and its genesis can be multiple-level hearsay, rumor, surmise, and speculation. Also, the motivation driving sources of raw intelligence to impart information is usually not nearly as transparent as in conventional criminal justice circumstances. As a result, the dangers of deception and disinformation are significantly enhanced.

#### ***b) Illegitimate and/or Illegal Sources of Information.***

There is also the danger that the information in FISA applications, whether or not attributed to a particular source, was generated by illegal means such as warrantless wiretapping or constitutionally infirm FAA surveillance that has not been affirmed by the U.S. Supreme

Court, or any circuit courts of appeal for that matter. In that context, the government should be compelled to disclose whether information in the FISA applications, or which was used to obtain information that appears in the applications, or was used in the investigation in this case in any fashion, originated from such illegitimate means. *See Gelbard v. United States*, 408 U.S. 41 (1972) (in prosecution for contempt for refusal to testify, grand jury witness entitled to invoke as a defense statutory bar against use of evidence obtained via illegal wiretap as basis for questions in grand jury).

***(1) The Warrantless Terrorist Surveillance Program.***

For example, the government should be required to disclose whether any of Defendant's communications were intercepted pursuant to the Terrorist Surveillance Program (hereinafter "TSP"), a warrantless wiretapping program instituted in 2001. *See In re National Security Agency Telecommunications Records Litigation (pertaining to: Al-Haramain Islamic Foundation, Inc. v. Bush)*, 451 F. Supp.2d 1215 (D. Ore. 2006), *rev'd and remanded*, 507 F.3d 1190 (9th Cir. 2007), *on remand to Northern District of California*, 564 F. Supp.2d 1109 (N.D. Cal. 2008), *after remand*, 700 F. Supp.2d 1182 (N.D. Cal. 2010). *See also ACLU v. National Security Agency*, 438 F. Supp. 2d 754 (E.D. Mich.2006), *rev'd on standing grounds*, 493 F.3d 644 (6th Cir. 2007). The government should further be compelled to disclose whether any communications intercepted pursuant to the TSP—whether or not Hendricks was a party—contributed to the FISA applications or the search warrant applications or to the investigation of this case in any manner .

**4. FISA's Prohibition of Basing Probable Cause Solely On a "United States Person's" Protected First Amendment Activity**

FISA includes an additional restriction for electronic surveillance of a “United States person,” as it prohibits finding probable cause for such a target based solely upon First Amendment activities. In making that probable cause determination, the statute directs “[t]hat no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the First Amendment.” §1805(a)(2)(A).

Accordingly, if the targeted individual participated in First Amendment activities such as expressing opinions online, commenting in web forums and chat rooms, or posting or commenting on others’ videos, such activities cannot serve as a basis for probable cause for a FISA warrant.

Based on the discovery received and reviewed thus far, Hendricks’ and unindicted co-conspirator’s online activities may have included such expressive behavior. Such expression clearly implicates First Amendment-protected conduct, no matter how repugnant that the government or even the general public may find it. *See Snyder v. Phelps*, 562 U.S. 443 (2011) (First Amendment protects picketers at military funeral). Activities such as expressing support, urging others to express support, gathering information, and distributing information are protected and cannot serve as a basis for probable cause. *See Nat’l Ass’n for Advancement of Colored People v. Button*, 371 U.S. 415, 444-45 (1963) (The “First Amendment protects expression and association without regard to the race, creed, or political or religious affiliation of the members of the group which invokes its shield, or to the truth, popularity, or social utility of the ideas and beliefs which are offered.”). Moreover, the First Amendment includes the freedom to advocate the use of force or the violation of the law or even to advocate for unlawful action at some indefinite time in the future. *See Brandenburg v. Ohio*, 395 U.S. 444, 447-49 (1969); *Hess*

*v. Indiana*, 414 U.S. 105, 108-09 (1973).

This, of course, begs the question whether there was any basis, other than protected First Amendment activity, for commencing FISA surveillance on Defendant or his co-defendants. Should the answer be in the negative, the FISA surveillance would be invalid under §1805(a)(2)(A). In any event, it is paramount that the adversary process be allowed to function in its full capacity in this case to ensure the enforcement of FISA's First Amendment protections, and that defense counsel be allowed to view all FISA applications and warrants and fully participate in challenging their validity.

**B. The FISA Applications May Contain Intentional or Reckless Falsehoods or Omissions in Contravention of *Franks v. Delaware*, 438 U.S. 154 (1978).**

The Supreme Court's landmark decision in *Franks v. Delaware*, 438 U.S. 154 (1978), established the circumstances under which the target of a search may obtain an evidentiary hearing concerning the veracity of the information set forth in a search warrant affidavit. As the Court in *Franks* instructed, "where the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statements are necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request." *Franks*, 438 U.S. at 156-57.

The *Franks* opinion also sets a similar standard for suppression following the evidentiary hearing:

[I]n the event that at that hearing the allegation of perjury or reckless disregard is established by the defendant by a preponderance of the evidence, and, with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking

on the face of the affidavit.

*Id.*, at 156; see *United States v. Blackmon*, 273 F.3d 1204, 1208-10 (9th Cir. 2001) (applying *Franks* to Title III wiretap application); *United States v. Meling*, 47 F.3d 1546, 1553-56 (9th Cir. 1995) (same); *United States v. Duggan*, 743 F.2d 59, 77 n.6 (2d Cir. 1984) (suggesting that *Franks* applies to FISA applications under Fourth and Fifth Amendments). See also *United States v. Hammond*, 351 F.3d 765, 770-71 (6th Cir. 2003) (applying *Franks* principles). The *Franks* principles apply to omissions as well as to false statements. See, e.g., *United States v. Carpenter*, 360 F.3d 591, 596-97 (6th Cir. 2004); *United States v. Atkin*, 107 F.3d 1213, 1216-17 (6th Cir. 1997). Omissions will trigger suppression under *Franks* if they are deliberate or reckless, and if the search warrant affidavit, with omitted material added, would not have established probable cause.

As noted above, without the opportunity to review the applications, counsel cannot point to or identify any specific false statements or material omissions in those applications. Although that lack of access prevents counsel from making the showing that *Franks* ordinarily requires, counsel note that the possibility that the government has submitted FISA applications with intentionally or recklessly false statements or material omissions is hardly speculative. For instance, in 2002, in *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 620-21 (FISC 2002), *rev'd on other grounds sub nom.*, *In re Sealed Case*, 310 F.3d 717 (FISCR 2002), the FISC reported that beginning in March 2000, the Department of Justice (hereinafter “DoJ”) had come “forward to confess error in some 75 FISA applications related to major terrorist attacks directed against the United States. The errors related to misstatements and omissions of material facts,” including:

- “75 FISA applications related to major terrorist attacks directed against the United States” contained “misstatements and omissions of material facts.” 218 F. Supp. 2d at 620-21;
- the government’s failure to apprise the FISC of the existence and/or status of criminal investigations of the target(s) of FISA surveillance. *Id.*; and,
- improper contacts between criminal and intelligence investigators with respect to certain FISA applications. *Id.*

According to the FISC, “[i]n March of 2001, the government reported similar misstatements in another series of FISA applications . . .” *Id.* at 621. Nor were those problems isolated or resolved by those revelations. Instead, they proved persistent. A report issued March 8, 2006, by the DoJ Inspector General stated that the FBI found apparent violations of its own wiretapping and other intelligence-gathering procedures more than 100 times in the preceding two years, and problems appear to have grown more frequent in some crucial respects. *See* Report to Congress on Implementation of Section 1001 of the USA PATRIOT Act, March 8, 2006 (hereinafter “DoJ IG Report”),

The report characterized some violations as “significant,” including wiretaps that were much broader in scope than authorized by a court (“over-collection”), and others that continued for weeks and months longer than authorized (“overruns”). *Id.* at 24-25. 15 FISA-related over-collection violations constituted 69% of the reported violations in 2005, an increase from 48% in 2004. *See* DoJ IG Report, at 29. The total percentage of FISA-related violations rose from 71% to 78% from 2004 to 2005, *id.*, at 29, although the amount of time “over-collection” and “overruns” were permitted to continue before the violations were recognized or corrected decreased from 2004 to 2005. *Id.* at 25.

Thus, a *Franks* hearing, and disclosure of the underlying FISA materials, are necessary in

order to permit counsel the opportunity to prove that the affiants before the FISC intentionally or recklessly made materially false statements and omitted material information from the FISA applications.

**C. The Collection of Foreign Intelligence Information Was Not a Significant Purpose of the FISA Surveillance.**

As set forth more fully in section VI, *infra*, in 2001 Congress amended the language of FISA which required that the collection of foreign intelligence information be “the purpose” of the collection, to a “a significant purpose”—greatly expanding the Intelligence Agencies’ ability to collect information pursuant to FISA. Nonetheless, the information collected pursuant to FISA be suppressed if a significant purpose of the search and collection was not foreign intelligence. In that Farooq and his co-defendant’s engaged in considerable First Amendment protected activity in the course of the charged conspiracy, and, the Court should order the government to disclose the FISA applications and related materials to allow the defense so as to determine that the acquisition of foreign intelligence was a significant purpose of the surveillance.

**D. The FISA Applications May Not Have Included the Required Certifications.**

The Court should review the FISA applications to determine whether they contain all certifications required by §1804(a)(6). As the Ninth Circuit has declared in the Title III context, “[t]he procedural steps provided in the Act require ‘strict adherence,’” and “utmost scrutiny must be exercised to determine whether wiretap orders conform to [the statutory requirement].” *Blackmon*, 273 F.3d at 1207, *quoting United States v. Kalustian*, 529 F.2d 585, 588-9 (9th Cir. 1975).

In addition, the Court should examine two certifications with particular care—(i) that the information sought is “the type of foreign intelligence information designated,” and (ii) that the

information “cannot reasonably be obtained by normal investigative techniques.” *See* § 1804(a)(6)(E). Particularly if the target of the wiretap is a “United States person” these two certifications must be measured by the “clearly erroneous” standard. *See* § 1805(a)(4). As the Ninth Circuit has observed in relation to the similar provision in Title III, 18 U.S.C. § 2518(1)(e), “the necessity requirement ‘exists in order to limit the use of wiretaps, which are highly intrusive.’” *Blackmon*, 273 F.3d at 1207, *quoting United States v. Bennett*, 219 F.3d 1117, 1121 (9th Cir. 2000) (internal quotation omitted). The necessity requirement “ensure[s] that wiretapping is not resorted to in situations where traditional investigative techniques would suffice to expose the [information sought].” *Id.*

The Court should also carefully examine the dates, in sequence, of all FISA orders in this case to determine whether there were any lapses of time during which wiretapping continued. The statutory scheme contemplates a seamless web: when a FISA order expires and the government wishes to continue the wiretap, the expiring order must be replaced by an extension order, which, in turn, may be obtained only on the basis of a proper FISA application. *See* § 1805(d)(1) & (2). FISA surveillance that continues past the expiration date of the FISA order that originally authorized it is just as unauthorized as a wiretap that is initiated without any FISA order at all. Should the Court order the government to disclose the FISA orders in this case to defense counsel, then counsel will be able to assist the Court in matching up all of the FISA orders by date—an arduous, albeit necessary, task.

**E. The FISA Applications, and the FISA Surveillance, May Not Have Contained or Implemented the Requisite Minimization Procedures.**

In order to obtain a valid FISA order, the government must include in its application a “statement of the proposed minimization procedures.” § 1804(a)(4). The purpose of these

minimization procedures is to: (i) ensure that surveillance is reasonably designed to minimize the acquisition and retention of private information regarding people who are being wiretapped; (ii) prevent dissemination of non-foreign intelligence information; and (iii) prevent the disclosure, use, or retention of information for longer than seventy-two hours unless a longer period is approved by Court order. § 1801(h).

As FISA involves particularly intrusive electronic surveillance, FISA interception is a “24/7” operation, as the Title III principle of “pertinence” is not applicable; instead, *all* conversations are captured, with minimization occurring later and in other forms, minimization in the FISA context is critically important. A court and commentator have reasoned that “[i]n FISA the privacy rights of individuals are ensured not through mandatory disclosure [of FISA applications,] but through its provisions for in-depth oversight of FISA surveillance *by all three branches of government* and by a statutory scheme that to a large degree centers on *an expanded conception of minimization* that differs from that which governs law-enforcement surveillance.” *United States v. Belfield*, 692 F.2d 141, 148 & n. 34 (D.C. Cir. 1982) (footnote omitted), *quoting* Schwartz, *Oversight of Minimization Compliance Under the Foreign Intelligence Surveillance Act: How the Watchdogs are Doing Their Job*, 12 RUTGERS L.J. 405, 408 (1981) (emphasis added). In order to determine whether there were adequate minimization procedures here, and that the government complied therewith, defense counsel should be provided with the FISA applications, orders, and related materials.

#### **IV. THE UNDERLYING FISA APPLICATIONS AND OTHER MATERIALS SHOULD BE DISCLOSED TO DEFENSE COUNSEL TO ENABLE THEM TO ASSIST THE COURT, AND ON DUE PROCESS GROUNDS**

##### **A. Disclosure of FISA Materials to the Defense Pursuant to §1806(f)**

So that counsel may fully develop the arguments articulated above in order to allow the Court to make a fully informed decision regarding suppression and also as to other critical issues, such as the production of *Brady* material, the Court should order that the FISA applications and orders be disclosed to defense counsel. According to FISA's legislative history, disclosure may be "necessary" under §1806(f):

[W]here the court's initial review of the application, order, and fruits of the surveillance indicates that the question of legality may be complicated by factors such as 'indications of possible misrepresentation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order.

*United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982); *see, e.g., United States v. Ott*, 827 F.2d 473, 476 (9th Cir. 1987) (same); *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984) (same).

Here, as discussed above, there are ample justifications for disclosure of the FISA applications, which would permit defense counsel an opportunity to demonstrate that the requisite probable cause was lacking—including specifically, that the information in the applications was either unreliable or obtained via illegal means. Disclosure would also afford defense counsel an opportunity to identify procedural irregularities.

In addition, any security concerns are addressed by the fact that undersigned counsel are completing obtaining a security clearance. It is understood no disclosures would or could be made until clearance has been confirmed. Further, this Court can issue an appropriate Protective Order, to which Defendant's counsel would of course consent, that would provide elaborate protection for CLASSIFIED information, and which would permit CLASSIFIED materials to be disclosed to defense counsel but not to Defendant. *See Classified Information Procedures Act*

(hereinafter “CIPA”), 18 U.S.C. App. III, at §3.

Thus, while only one court in the thirty-eight (38) year history of FISA has ordered disclosure of FISA applications, orders, or related materials, the circumstances herein compel disclosure. Moreover, the existence of § 1806(f) is an unambiguous declaration that Congress intended for courts to grant disclosure in appropriate cases. If § 1806(f) is to be rendered meaningful at all, and not be rendered superfluous and entirely inert, it should apply in this case.

**B. Disclosure of FISA Materials to the Defense Pursuant to §1806(g).**

Even if the Court were to decline to find that disclosure of FISA-related materials to the defense is appropriate under §1806(f), the defense would still be entitled to disclosure of the FISA applications, orders, and related materials under §1806(g), which expressly incorporates the Fifth Amendment Due Process Clause, and provides that “[i]f the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person *except to the extent that due process requires discovery or disclosure.*” 50 U.S.C. §1806(g) (emphasis added). *See also United States v. Spanjol*, 720 F. Supp. 55, 57 (E.D. Pa. 1989) (“[u]nder FISA, defendants are permitted discovery of materials only to the extent required by due process. That has been interpreted as requiring production of materials mandated by [*Brady*], essentially exculpatory materials”).

**C. Ex Parte Proceedings are Antithetical to the Adversary System of Justice.**

Lack of disclosure would render the proceedings on the validity of the FISA surveillance *ex parte*, as the challenges on Defendant’s behalf would be made without access to documents and information essential to the determination of his motion. Such proceedings are antithetical to the adversary system that is the hallmark of American criminal justice. *Ex parte* proceedings

impair the integrity of the adversary process and the criminal justice system. As the Supreme Court has recognized, “[f]airness can rarely be obtained by secret, one-sided determination of facts decisive of rights. . . . No better instrument has been devised for arriving at truth than to give a person in jeopardy of serious loss notice of the case against him and opportunity to meet it.” *United States v. James Daniel Good Real Property, et. al.*, 510 U.S. 43, at 55 (1993) (quoting *Joint Anti-Fascist Refugee Committee v. McGrath*, 341 U.S. 123, 170-72 (1951)). See also *United States v. Madori*, 419 F.3d 159, 171 (2d Cir. 2005), citing *United States v. Arroyo-Angulo*, 580 F.2d 1137, 1145 (2d Cir.1977) (closed proceedings “are fraught with the potential of abuse and, absent compelling necessity, must be avoided”) (other citations omitted).

In *United States v. Abuhamra*, 389 F.3d 309 (2d Cir. 2004), the Second Circuit reemphasized the importance of open, adversary proceedings, declaring that “[p]articularly where liberty is at stake, due process demands that the individual and the government each be afforded the opportunity not only to advance their respective positions but to correct or contradict arguments or evidence offered by the other.” *Abuhamra*, 389 F.3d at 322-23 [citing *McGrath*, 341 U.S. at 171 n. 17 (Frankfurter, J., *concurring*)] (noting that “the duty lying upon everyone who decides anything to act in good faith and fairly listen to both sides . . . always giving a fair opportunity to those who are parties in the controversy for correcting or contradicting any relevant statement prejudicial to their view”) (citation and internal quotation marks omitted).

As the Ninth Circuit observed in the closely analogous context of a secret evidence case, “[o]ne would be hard pressed to design a procedure more likely to result in erroneous deprivations. . . . [T]he very foundation of the adversary process assumes that use of undisclosed

information will violate due process because of the risk of error.” *American-Arab Anti-Discrimination Committee v. Reno*, 70 F.3d 1045, 1069 (9th Cir. 1995) (quote marks omitted); *Kiareldeen v. Reno*, 71 F. Supp. 2d 402, 412-14 (D. N.J. 1999) (same).

Similarly, in the Fourth Amendment context, including in relationship to electronic surveillance, the Supreme Court has twice rejected the use of *ex parte* proceedings on grounds that apply equally here. In *Alderman v. United States*, 394 U.S. 165 (1969), the Court addressed the procedures to be followed in determining whether government eavesdropping in violation of the Fourth Amendment contributed to the prosecution case against the defendants. The Court rejected the government’s suggestion that the district court make that determination *in camera* and/or *ex parte*. The Court observed:

[a]n apparently innocent phrase, a chance remark, a reference to what appears to be a neutral person or event, the identity of a caller or the individual on the other end of a telephone, or even the manner of speaking or using words may have special significance to one who knows the more intimate facts of an accused’s life. And yet that information may be wholly colorless and devoid of meaning to one less well acquainted with all relevant circumstances.

*Id.* at 182. And in ordering disclosure of improperly recorded conversations, the Court declared: [a]dversary proceedings will not magically eliminate all error, but they will substantially reduce its incidence by guarding against the possibility that the trial judge, through lack of time or unfamiliarity with the information contained in and suggested by the materials, will be unable to provide the scrutiny that the Fourth Amendment exclusionary rule demands.

*Id.* at 184.

Likewise, the Supreme Court held in *Franks*, that a defendant, upon a preliminary showing of an intentional or reckless material falsehood in an affidavit underlying a search warrant, must be permitted to attack the veracity of that affidavit. The Court rested its decision in

significant part on the inherent inadequacies of the *ex parte* nature of the procedure for issuing a search warrant, and the contrasting enhanced value of adversarial proceedings:

[T]he hearing before the magistrate [when the warrant is issued] not always will suffice to discourage lawless or reckless misconduct. The pre-search proceeding is necessarily *ex parte*, since the subject of the search cannot be tipped off to the application for a warrant lest he destroy or remove evidence. The usual reliance of our legal system on adversary proceedings itself should be an indication that an *ex parte* inquiry is likely to be less vigorous. The magistrate has no acquaintance with the information that may contradict the good faith and reasonable basis of the affiant's allegations. The pre-search proceeding will frequently be marked by haste, because of the understandable desire to act before the evidence disappears; this urgency will not always permit the magistrate to make an independent examination of the affiant or other witnesses.

438 U.S. at 169.

The same considerations that the Supreme Court found compelling in *Alderman* and *Franks* militate against *ex parte* procedures in the FISA context. Indeed, the lack of any authentic adversary proceedings in FISA litigation more than likely accounts for the government's perfect record in defending FISA and FISA-generated evidence. After all, denying an adversary access to the facts constitutes an advantage as powerful and insurmountable as exists in litigation.

As the FISC itself has acknowledged, for example, without adversarial proceedings, systematic executive branch misconduct—including submission of FISA applications with “erroneous statements” and “omissions of material facts”—went entirely undetected by the courts until the FISC directed that the Department of Justice review FISA applications and submit a report to the FISC. *See In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp.2d at 620-21, *rev'd on other grounds*, 310 F.3d 717 (FISCR 2002).

However, as discussed above, the complete deference now required of the courts toward the executive with respect to FISA renders any such “in-depth oversight” and “expanded conception of minimization” (relied upon in *Belfield*, 692 F.2d at 148 & n. 34) entirely illusory. As a result, §§1806(f) & (g), and the disclosure they authorize, assume significantly greater meaning and importance in evaluating the validity of FISA applications. Also, as noted above, defense counsel Durkin possesses the requisite security clearance to view the material, thereby further eliminating any justification for non-disclosure, or any claim that such limited, safe disclosure presents any danger to national security.

Finally, the Court’s review *in camera* is not a substitute for defense counsel’s participation. As the Supreme Court recognized in *Alderman*, “[i]n our adversary system, it is enough for judges to judge. The determination of what may be useful to the defense can properly and effectively be made only by an advocate.” 394 U.S. at 184. Accordingly, either under §1806(f), §1806(g), and/or the Due Process clause, disclosure of the FISA materials is authorized and appropriate in this case.

**V. WHETHER OR NOT THE COURT ORDERS DISCLOSURE SO THAT COUNSEL MAY MEANINGFULLY PARTICIPATE FOR THE MOTION TO SUPPRESS, THIS COURT'S REVIEW OF THE FISA WARRANT OR WARRANTS IS *DE NOVO*.**

The Court should review the FISA applications and orders *de novo*. *United States v. Hammoud*, 381 F.3d 316, 332 (4th Cir. 2004) (noting district court's *de novo* review and conducting its own *de novo* review of FISA materials), *vacated on other grounds*, 543 U.S. 1097 (2005); *United States v. Squillacote*, 221 F.3d 542, 554 (4th Cir. 2000) (same); *see also United States v. Campa*, 529 F.3d 980, 991 (11th Cir. 2008); *United States v. Kashmiri*, 2010 U.S. Dist. LEXIS 119470, \*4 (N.D. Ill. Nov. 10, 2010) ("The court conducts a *de novo* review of the FISA materials to determine if the electronic surveillance authorization was based upon appropriate probable cause.")

Courts have held that a reviewing court is to conduct essentially the same review of the FISA application and associated materials that the FISC conducted upon receiving an application requesting a FISA order. *See, e.g., In re Grand Jury Proceedings of Special April 2002 Grand Jury*, 347 F.3d 197, 204-05 (7th Cir. 2003). Accordingly, the court reviews, first, the adequacy of the FISA materials at issue "*de novo* with no deference accorded to the FISC's probable cause determinations," and second, the Executive Branch's certifications, which are reviewed for clear error. *United States v. Rosen*, 447 F. Supp. 2d 538, 545 (E.D. Va. 2006).

Robust *de novo* review is all the more important if meaningful defense participation in the suppression motion is not permitted, and the government's assertions could thus be untested by the adversarial process. Moreover, there is reason for this Court's review to be more exacting than the FISC's review of the government's applications for a FISA order. Unlike the FISC applications, the FISA activity is no longer about intelligence gathering, but is now being used to

seek a conviction and imprisonment. The focus should therefore now be on the rights of the defendant, rather than simply general interests in intelligence gathering.

The Court should also be cognizant of its role as a neutral and detached arbiter, and the distinct separation of powers at issue here. The role of a FISC judge is significantly different than that of an ordinary judge or magistrate because the statute directs deference to the Executive Branch's certifications and also because the FISA applications and orders are shrouded in almost complete secrecy.

**VI. SHOULD THE COURT NOT ALLOW DEFENSE COUNSEL'S PARTICIPATION REGARDING FISA SEARCHES AND SEIZURES, THE COURT SHOULD ALSO CONSIDER POTENTIAL FISA'S CONSTITUTIONAL VIOLATIONS, BOTH FACIALLY AND AS APPLIED IN THIS CASE.**

Review of the issues raised by Defendant's motion to suppress and for disclosure requires the Court to engage in interpretation and construction of a number of provisions of FISA. At a minimum, the following provisions are necessarily called into question. To the extent the government disagrees with counsel's interpretations of those provisions, or the Court is inclined to side with some of the Circuits that have read the statute more broadly, review in this case will require consideration of the constitutionality of the statute itself. There are a number of reasons why a broad reading of FISA, particularly as amended by the Patriot Act, could be said to violate the First, Fourth, Fifth, and Sixth Amendments. As in all cases, the Court's review should proceed under the basic rule of statutory construction that where a plausible reading of a statute would avoid serious constitutional problems, the Court should follow that construction instead of a construction that raises serious constitutional issues. *See Skilling v. United States*, 561 U.S. 358, 423 (2010).

To the extent the Court does not narrowly read the FISA statute, the procedures it

purports to authorize should be found to violate the Constitution. Prior to the enactment of FISA, and for the first twenty-five (25) years of its existence, the “primary purpose” for surveillance or searches was required to be intelligence gathering with respect to a “foreign power” or an “agent of a foreign power.” *United States v. Truong Dinh Hung*, 629 F.2d 908, 912-13 (4th Cir. 1980); 50 U.S.C. § 1805(a)(3) (2000). The non-criminal purpose standard was essential to the cases upholding FISA’s constitutionality. Courts refined the statutory standard and held that FISA-generated evidence was admissible so long as the government’s “primary purpose” in conducting the electronic surveillance was the gathering of foreign intelligence information—as opposed to information to build a criminal investigation of the target of the eavesdropping or search. *See, e.g., United States v. Duggan*, 743 F.2d 59, 77 (2d Cir. 1984).

However, in October 2001, through the Patriot Act, Congress, without any debate, amended the language of FISA and changed the language requiring that “*the purpose*” of the search or surveillance to be the acquisition of foreign intelligence information, to requiring that such acquisition be “a significant purpose.” 50 U.S.C. § 1804(a)(7)(B) and § 1823(a)(7)(B) (as amended by Pub.L. 107-56, Title II, § 218, Oct. 26, 2001) (emphasis added). *See also In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611 (FISA 2002), *reversed in part, In re Sealed Case*, 310 F.3d 717 (FISA Rev. 2003). These Patriot Act amendments dramatically expanded the class of investigations in which FISA is available to the government, and have enabled the government to conduct surveillance to gather evidence for use in a criminal case without a traditional warrant—so long as the government can state that there is a “significant purpose” in gathering foreign intelligence.

Thus, while FISA set out to reduce the probable cause requirement only for national

security intelligence gathering, a consequence, intended or not—of the Patriot Act has been that the Executive Branch may now “bypass the Fourth Amendment” to gather evidence for a criminal prosecution. *See Mayfield v. United States*, 504 F. Supp. 2d 1023, 1036-37 (D. Ore. 2007) (holding FISA as amended to be unconstitutional), *vacated and remanded on other grounds*, 599 F.3d 964 (9th Cir. 2010) (plaintiff lacked standing due to settlement agreement with government).

While courts have found that the reduced “significant purpose” standard does not violate the Constitution, there has been no such ruling after the widely publicized public disclosures regarding the expansive nature of Section 702’s PRISM and Upstream collections, particularly insofar as they involve the collection of domestic communications of American citizens. This is significant due to the history of FISA and the approval of the “significant purpose” standard based on the rationale that the purpose, whether significant or primary, was still the gathering of foreign intelligence regarding a foreign power or agent of a foreign power. *See, e.g., United States v. Pelton*, 835 F.2d 1067, 1075- 76 (4th Cir. 1987); *United States v. Badia*, 827 F.2d 1458, 1464 (11th Cir. 1987).

The fact we now know that NSA surveillance programs essentially vacuum-up an untold number of domestic communications calls into question the very underpinnings of such prior decisions. No longer can it simply be naively accepted that the purpose of FISA surveillance is foreign intelligence—no matter how disagreeable the government may find the content of those postings.

In *United States v. United States District Court (Keith)*, 407 U.S. 297 (1972), the Court rejected the government’s contentions that national security investigations are too complex for

judicial evaluation, and that requiring prior judicial approval would fracture secrecy essential to official intelligence gathering. *Id.* at 318-21. The Supreme Court also rejected the government's argument that exceptions to the Fourth Amendment warrant requirement should be recognized for domestic security surveillance. *Id.* at 316-17.

The Supreme Court further warned that “[t]he historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.” *Id.* at 316-17. *See also United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991) (stating that “the investigation of criminal activity cannot be the primary purpose of the surveillance,” and that FISA may “not be used as an end-run around the Fourth Amendment’s prohibition of warrantless searches”). The Supreme Court’s warning now seems prescient.

It appears now that through virtually unchecked NSA surveillance programs that until recently operated in near secrecy, the government has—under the auspices of FISA and more likely the FAA—engaged in the domestic surveillance forbidden by *Keith*, and traditional First and Fourth Amendment jurisprudence. If the government used FISA or the FAA in such a manner in this case, then the Court should find its application unconstitutional and suppress any and all evidence obtained as a result of such surveillance.

This case presents the unique and historical opportunity for the Judicial Branch to exercise its time-honored authority to put a stop to unfettered and unconstitutional Executive Branch covert activity, the very activity FISA was designed to correct.

## II. CONCLUSION

For all of the above reasons, the motion to suppress should be granted.

Respectfully submitted,

S/ David L. Doughten  
David L. Doughten

S/ Steven D. Hartman  
Stephen D. Hartman

Counsel for Defendant Hendricks

7